EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John Fitzgerald on 6/2/2009.

The application has been amended as follows beginning on the following page:

1. (Currently amended) A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps ~~at the server of~~:

receiving the message [[at]] by the server from the sender;

generating [[at]] by the server a digital signature of the message;

generating [[at]] by the server a file containing, in HTML format, an identity of the sender and instructions describing how to authenticate the message;

concealing the digital signature of the message in the file;

attaching the file containing the identity of the sender and instructions describing how to authenticate the message and the concealed digital signature to the message [[at]] by the server;

transmitting from the server to the recipient the message and the attachment;

receiving the message and the attachment [[at]] by the server from the recipient;

providing digital signatures of the message and the attachment [[at]] by the server, and

authenticating to the recipient the message and the attachment [[at]] by the server on the basis of the information received by the recipient from the server and on the basis of the digital signatures provided by the server.

2. (Original) A method as set forth in claim 1 wherein the server creates digital fingerprints from the digital signatures and from the message and the attachment to authenticate the message and the attachment on the basis of the digital fingerprints.

3. (Previously presented) A method as set forth in claim 1 wherein the attachment includes interim stations between the recipient and the server and wherein

the message and the attachment, and the digital signatures of the message and the attachment, are transmitted from the server to the sender to provide for a determination at the server for the sender of the authenticity of the message and the attachment.

4. (Original) A method as set forth in claim 3 wherein the message and the attachment and the digital signatures of the message and the attachment are not retained at the sender when the message and the attachment and the digital signatures are transmitted from the server to the sender.

5. (Original) A method as set forth in claim 1 wherein the message and the attachment and the digital signatures of the message and the attachment are transmitted from the server to the sender.

6. (Original) A method as set forth in claim 5 wherein

the sender transmits to the server, to authenticate the message, the information supplied by the server to the sender and wherein

the server operates upon the information from the sender to authenticate the message.

7. (Original) A method as set forth in claim 5 wherein the message and the digital signature of the message are discarded after the message and the digital signature are transmitted by the server to the sender.

8. (Currently amended) In a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps at the ~~server~~ of:

receiving the message from the sender;

generating [[at]] by the server a digital signature of the message;

generating at the server an attachment which contains an identity of the sender and instructions on how to authenticate the message in HTML format, and the digital signature of the message, the digital signature being concealed in the attachment;

transmitting the message and the attachment from the server to the recipient;

receiving the message and the attachment at the server from the recipient;

providing digital fingerprints of the message and the digital signature of the message and digital fingerprints of the attachment and the digital signature of the attachment; and;

comparing the digital fingerprints at the server to determine the authenticity of the message.

9. (Currently amended) In a method as set forth in claim 8, the steps ~~at the server~~ of:

transmitting to the recipient the state of authenticity of the message on the basis of the results of the comparison of the digital fingerprints.

10. (Currently amended) In a method as set forth in claim 1, the steps ~~at the server~~ of:

receiving ~~at the server from the recipient~~ the message and the attachment from the recipient by the server;

receiving from the sender the message and the attachment and the digital signatures of the message and the attachment;

producing digital fingerprints of the message, the attachment and the digital signatures; and

comparing the digital fingerprints relating to the message, and the digital fingerprints relating to the attachment, to determine the authenticity of the message and the attachment.

11. (Currently amended) In a method as set forth in claim 10, the steps ~~at the server~~ of:

disposing of the message and the attachment and the digital signatures of the message and the attachment after transmitting this information to the sender.

12. (Currently amended) In a method as set forth in claim 5, the steps ~~at the server~~ of:

providing at the server, at the same time as the reception of the message, an attachment including the identity of the sender and the identity and address of the server and

the identity and address of the recipient and the time of transmission of the message from the server to the recipient;

transmitting from the server to the recipient the attachment at the same time as the transmission of the message;

receiving from the recipient at the server the message and the attachment;

providing digital fingerprints of the message, the attachment and the digital signatures of the message and the attachment; and

providing an indication of the authentication of the attachment on the basis of a comparison at the server of the digital fingerprints relating to the message and the digital fingerprints relating to the attachment.

13. (Currently amended) In a method as set forth in claim 12, the step ~~at the server~~ of:

transmitting from the server to the recipient an indication of the authenticity of the message on the basis of the comparison of the digital fingerprints relating to the message and the digital fingerprints relating to the attachment.

14. (Currently amended) A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps ~~at the server~~ of:

receiving the message at the server from the sender;

generating a digital signature of the message at the server;

providing [[at]] by the server, at the same time as the reception of the message [[at]] by the server, an attachment including the identity of the sender and instructions of how to authenticate the message and the identity and address of the recipient and the time of transmission of the message and the digital signature of the message in HTML format, the digital signature of the message being concealed in the attachment;

providing a digital signature of the attachment at the server;

sending the message and the attachment to the recipient;

receiving from the recipient the message and the attachment; and

determining the authenticity of the message and the attachment at by the server from the message and the attachment at the server and the digital signatures at the server of the message and the attachment.

15. (Currently amended) A method as set forth in claim 14 wherein

digital fingerprints are provided [[at]] by the server of the message and the attachment and digital fingerprints are provided [[at]] by the server of the digital signatures of the message and the attachment and wherein

a comparison is provided [[at]] by the server of the digital fingerprints of the message and the digital signature of the message, and the attachment and the digital signature of the attachment, to determine the authenticity of the message and the attachment.

16. (Currently amended) A method as set forth in claim 15 wherein

the indications of the state of authenticity of the message and the attachment are transmitted from the server to the recipient and wherein

the message and the attachment and the digital signatures of the message and the attachment are discarded [[at]] by the server when the indications of the authenticity of the message and the attachment are transmitted from the server to the recipient.

17. (Original) A method as set forth in claim 14 wherein

the message and the attachment and the digital signatures of the message and the attachment are transmitted from the server to the sender and wherein

the server produces digital fingerprints of the message and the attachment and digital fingerprints of the digital signature of the message and the attachment and wherein

the server compares the digital fingerprints relating to the message, and the digital fingerprints relating to the attachment, to determine the authenticity of the message and the attachment.

18. (Original) A method as set forth in claim 17 wherein

the server transmits to the recipient the results of the comparison and wherein

the server discards the message and the attachment and the digital signatures of the message and the attachment when the server transmits the message and the attachment and the digital signature of the message and the attachment to the recipient.

19. (Currently amended) In a method as set forth in claim 1 wherein

the message is received [[at]] by the server through an internet and wherein

the message and the digital signature of the message are transmitted to the recipient through the internet.

20. (Original) In a method as set forth in claim 19 wherein

the state of authenticity of the message is transmitted through the internet to the recipient.

21. (Previously presented) In a method as set forth in claim 8 wherein

the message from the sender is received at the server through an internet and wherein

the message is transmitted to the recipient through the internet.

22. (Original) In a method as set forth in claim 21 wherein

the state of authenticity of the message is transmitted from the server to the recipient through the internet.

23. (Previously presented) In a method as set forth in claim 14 wherein

the message is transmitted from the sender to the server through an internet and wherein

the message and the attachment are transmitted from the server to the recipient through the internet and wherein

the indication of the state of authenticity of the message and the attachment are transmitted from the server to the recipient through the internet.

24. (Currently amended) In a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps ~~at the server~~ of:

receiving a message from the recipient at a web site provided by the server, the message including an attachment containing an identity of a sender of the message, a concealed digital signature of the message and instructions on how to authenticate the message in HTML format ~~from the recipient at a web site providing at the server for~~ to obtain an indication of the authenticity of the message;

providing [[at]] by the server a compressed encrypted version of the message where the compression is a particular compression and the encryption is a particular encryption;

decompressing the message in accordance with the particular compression to provide a first digital fingerprint of the message;

decrypting the compressed encrypted version of the message in accordance with the particular encryption to provide a second digital fingerprint of the message; and

comparing the first and second digital fingerprints of the message to determine the authenticity of the message.

25. (Canceled)

26. (Previously presented) In a method as set forth in claim 24, the steps at the server of:

receiving the message through an internet from the recipient; and

transmitting the results of the comparison of the first and second digital fingerprints to the recipient through the internet.

27. (Currently amended) In a method of transmitting a message from a sender to a recipient through a server displaced from the recipient, the steps ~~at the server~~ of:

receiving a message from the recipient at a website providing [[in]] by the server for an indication of the authenticity of the message;

providing a compressed encrypted version of the message where the compression is a particular compression and the encryption is a particular encryption;

receiving an attachment separate from the message from the recipient at the website where the reception of the attachment is at the same time as the reception of the message and the attachment is in the form of an HTML file and contains information about delivery of the message to the recipient and a digital signature of the message concealed in the HTML file and instructions on how to authenticate the message;

providing a compressed encrypted version of the message where the compression is the particular compression and the encryption is the particular encryption;

decompressing the message and the attachment in accordance with the particular compression to provide first digital fingerprints of the message and the attachment;

decrypting the compressed encrypted versions of the message and the attachment in accordance with the particular encryption to provide second digital fingerprints of the message and the attachment; and

comparing the first and second digital fingerprints of the message, and the first and second digital fingerprints of the attachment, to determine the authenticity of the message and of the attachment.

28. (Currently amended) In a method as set forth in claim 27, the step ~~at the server~~ of:

transmitting to the recipient the results of the comparison of the first and second digital fingerprints of the message and the first and second digital fingerprints of the attachment.

29. (Canceled)

30. (Currently amended) In a method as set forth in claim 27, including the steps ~~at the server of~~:

receiving the message and the attachment through an internet from the recipient; and

transmitting the results of the comparison of the first and second digital fingerprints of the message, and the comparison of the first and second digital fingerprints of the attachment, to the recipient through the internet.

31. (Currently amended) In a method as set forth in claim 28, the steps ~~at the server~~ of:

transmitting to the recipient through an internet the results of the comparison of the first and second digital fingerprints of the message and the first and second digital fingerprints of the attachment.

32. (Original) In a method as set forth in claim 27 wherein

the attachment includes the identity of the sender and the identity and the address of the server and the identity and address of the recipient and the time of transmission of the message from the server to the recipient.

33. (Currently amended) In a method of transmitting a message from a sender through a server displaced from the recipient, the steps ~~at the server~~ of:

receiving the message and an attachment in the form of an HTML file that is not part of the message from the recipient at a website providing [[at]] by the server for an indication of the authenticity of the message, the attachment including an instruction on how to authenticate the message and a digital signature of the message, the digital signature of the message being concealed in the attachment;

providing [[at]] by the server for a compressed encrypted version of the combination of the message and the attachment where the compression is a particular compression and the encryption is a particular compression;

decompressing the compressed encrypted version of the combination of the message and the attachment in accordance with the particular compression to provide a first digital fingerprint of the combination of the message and the attachment;

decrypting the compressed encrypted version of the combination of the message and the attachment in accordance with the particular encryption to provide a second digital fingerprint of the combination of the message and the attachment; and

comparing the first and second digital fingerprints to determine the authenticity of the message and the attachment.

34. (Currently amended) In a method as set forth in claim 33, the step ~~at the server~~ of:

transmitting to the recipient the results of the comparison of the first and second digital fingerprints.

35. (Currently amended) In a method as set forth in claim 34, the steps at the server of:

receiving the message and the attachment, and the compressed encrypted version of the combination of the message and the attachment, through an internet; and

transmitting the results of the comparison of the first and second digital fingerprints to the recipient through the internet.

36. (Original) In a method as set forth in claim 33 wherein

the attachment includes the identity of the sender and the identity and the address of the server and the identity and address of the recipient and the time of the transmittal of the message to the recipient.

37. (Currently amended) In a method as set forth in claim 35, the steps at the server ~~of~~:

transmitting to the recipient the results of the comparison of the first and second digital fingerprints and wherein

the attachment includes the identity of the sender and the identity and the address of the server and the identity and address of the recipient and the time of the transmittal from the server to the recipient.

38. (Currently amended) In a method of transmitting a message and an attachment from a sender to a recipient through a server displaced from the recipient, including the steps at ~~the server~~ of:

identifying the sender;

hashing the attachments;

stripping the message of the attachments;

hashing the identification of the sender, the hashed attachments and the message to form a hashed string;

hashing the hashed string;

encrypting the hashed string after the hashing of the hashed string; and

digitally sealing the encrypted hash of the hashed string by attaching the encrypted hash of the hashed string to an HTML file containing instructions on how to authenticate the message and attaching the HTML file including the encrypted hash of the hashed string to the message and concealing the encrypted hash of the hashed string in the HTML file.

39. (Previously presented) In a method as set forth in claim 38, the steps of:

transmitting the message and the encrypted hash of the hashed string to the recipient.

40. (Currently amended) In a method of transmitting a message and an attachment from a sender through a server displaced from the recipient, the steps at the server of:

identifying the sender;

providing the attachment and the message stripped of the attachment;

providing a string formed from the identification of the sender, the attachment and the message stripped of the attachment; and

hashing the string;

encrypting the hash of the hashed string;

digitally sealing the encrypted hash of the hashed string by attaching the encrypted hash of the hashed string and instructions on how to authenticate the message to an HTML file and concealing the encrypted hash of the hashed string in the HTML file; and

sending to the recipient the message and the HTML file including the encrypted hash of the hashed string.

Claims 41-47 (Canceled)

The following is an examiner's statement of reasons for allowance:

The closest prior art, WO 01/10090, taught a server receiving a message from a sender, generating a digital signature of the message, attaching the identity of the sender, and the digital signature to the message, transmitting the message and attachment to the recipient, receiving the message and the attachment from the recipient, providing digital signatures of the message and the attachment at the server, and authenticating to the recipient the message and the attachment by the server on the basis of the information received by the recipient from the server and on the basis of the digital signatures provided by the server. What the prior art does not teach, is in combination with specific limitations as claimed, an HTML attachment or file containing instructions describing how to authenticate the message and concealing the digital signature in the file; and sending the message and file to the recipient, and/or receiving the message and the file by the server from the recipient.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571)272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2431